ABSTRACT

A method for providing secure access to information held in a shared repository, for example to electronic business cards stored on a server. A data owner registers with the server and provides information to be shared with selected data users. The server returns public-key cryptography keys. To access the information, a data user sends its public key to the data owner. The data owner encrypts the public key using the data owner private key, and sends the result to the server, along with permission to transfer information to the data user. The server decrypts the received result using the data owner public key, and compares the outcome with the data user public key. If they match, the server records permission on an access list. In response to a request for information the server checks the access list to determine whether the data user has permission. If so, the server encrypts the information using the data user public key, and transfers the result to the data user.